DEPARTMENT OF THE ARMY
UNITED STATES ARMY INTELLIGENCE AND SECURITY COMMAND
501ST MILITARY INTELLIGENCE BRIGADE
UNIT 15282
APO AP 96205-5282

JUL 25 2014

IADK-Z

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Brigade Policy Letter #23 – Network Security Violations

1. References:

a. AR 25-2 (Information Assurance) 24 October 2007.

c. INSCOM Policy Memorandum #64 (Information Assurance) 14 November 2012.

d. INSCOM Policy Memorandum #35 (Unauthorized Disclosure of Classified Information (UDCI) and Incident Handling and Response) 22 February 2013.

e. 501st Military Intelligence Brigade S6 Standard Operating Procedures (SOP).

2. Purpose. To implement a program to eliminate network security violations (NSV) represented by Negligent Discharges of Classified Information (NDCIs or spillage) and Cross Domain Violations (CDVs). Network Security Violations not only places the mission at risk, but careers as well. While enforcement of security policies for security measures will never ensure a 100% solution, implementation can drastically minimize the effects of unauthorized access of loss to information systems and the networks on which the information systems operate. Remember it takes the entire team to enforce Cyber Vigilance.

3. Summary. Our security is being compromised by an increasing number of network security violations, indicating a command-wide lack of understanding of the threats associated with improper handling of classified information on computer systems. The exposure of our sensitive and classified information puts the mission at risk and interrupts the continuity and capability of our networks. In addition to mission risk, countless man-hours are diverted for investigation and mitigation efforts. This is an unnecessary risk and an unacceptable loss of service that is completely avoidable.

4. Applicability.

a. Commanders will ensure personnel are in compliance with this policy.

b. This policy is directive in nature and will remain in effect until otherwise superseded or rescinded by regulation or other appropriate means. This policy and guideline applies to:

(1) Organizations. This policy applies to Headquarters staff elements, special staff, subordinate commands, tenant organizations, KATUSAs, ROK Army staff, DoD contractors, and civilians using or interfacing government information systems and networks regardless of location.

(2) Technologies and Classifications. This policy applies to all information technologies that are used to input, process, store, display or transmit information, regardless of classification or sensitivity.

5. Definitions.

a. Cross Domain Violation. Any instance in which an unaccredited or unauthorized information system or device is placed on a network. CDV examples include:

(1) Classified domain to unclassified domain (i.e. connecting a SIPR device to the NIPR);

(2) Unclassified domain to classified domain (i.e. connecting a NIPR device to SIPR);

(3) Any security domain to a different security domain (i.e. connecting a SIPR device to CENTRIX-K); and

(4) Use of unauthorized removal storage media, charging of privately portable electronic devices (PEDs), to include iPod/iPhone, MP3 players, privately owned Personal Digital Assistants (PDAs) and Blackberry, or using a SIPR laptop to configure multiple network devices.

b. Portable Electronic Devices (PEDs) are laptop computers, iPod/iPhone, Blackberry, or PDAs.

c. Removable Storage Media (RSM) include thumb drives (i.e. memory sticks, flash drives, Universal Serial Bus (USB) drives, pen drives, removable desktop or external USB hard drives, PCMCIA media, floppy disks, CD/DVD, photo flash cards that can store data or any other electronic media that can be attached to, inserted in, plugged into or connected via USB, firewire or wirelessly to a computer or Information System for the purpose of storing and/or transmitting data.

6. Policy.

a. Network Security Violations include a broad-category of events that include, but are not limited to:

(1) The mishandling or exposure of classified information on lower classified networks;

(2) Improper or unauthorized data transfers between systems or networks reported as Cross Domain Violations (CDVs);

(3) Attempts to use or attach equipment or devices not authorized for connection to DoD networks;

(4) Unauthorized attempts to access, collect or harvest data for which an individual does not possess the appropriate clearance level; and

(5) Any deliberate attempts to circumvent network access controls designed to protect sensitive or classified information.

b. Use of privately Portable Electronic Devices and/or Removable Storage Media on DoD networks is explicitly prohibited, except in limited instances indicated in AR 25-2, paragraph 4-30.b., sensitive DoD related information will not be stored on privately owned dev ices or storage media except when authorized.

c. Additional Removable Storage Media devices that are prohibited from connecting to DoD networks include the following: iPod/iPhone, MP3 players, privately owned PDA and Blackberrys.

d. All authorized mobile computing devices and removable media will be encrypted using an approved Data-at-Rest (DAR) solution approved by either the Brigade S6 OIC or the Brigade Information Assurance Manager (IAM).

e. All authorized Removable Storage Media must be marked with the appropriate level of classification using the GSA Standard Form sticker (SF 710, SF 707). Once utilized on a specific network, i.e., NIPR, SIPR, CENTRIXS-K, etc., devices must be marked appropriately and used only on the specified network.

f. Government removable storage media will be:

(1) Identified by classification label and serial number at the Information Management Officer (IMO) level.

(2) Approved for connectivity to DoD networks by submitting a Removable Storage Media Connection Request memorandum to the G6 Information Assurance Manager.

g. Computing devices to include removable storage media that can visibly label the device stating the device is authorized for travel and protected by a DAR Solution will be affixed.

h. Commanders and organizational leaders will ensure individuals have proper courier orders when traveling with classified PEDs or RSMs.

i. Commanders, organizational leaders, and staff sections will ensure the proper accountability and inventory of all devices and media that store sensitive, non-releasable, and classified information on them. Unit IMOs will develop a tracking mechanism that includes the following information to ensure proper accountability and inventory of these items:

(1) User's name, rank, command/section, and contact information.

(2) Serial/ID number, device type, and classification level at which it is used.

j. Procedural Security.

(1) Users will implement physical security measures IAW DoD Directive 5200.28 for portable electronic media to prevent loss, damage, or unauthorized access. Any loss of personally identifiable information, sensitive, classified, or non-expendable devices, or media will be reported immediately through the chain of command.

(2) Commanders and organizational IMOs will ensure devices and media are protected at the equivalent classification level of data stored/transmitted on it. Execute device and media physical security handling requirements identical to those of sensitive and classified hard copy documents.

(3) Commanders will enforce the use of double-wrapping and courier cards or orders for the mailing and/or transportation of classified devices and media outside of the installation.

(4) Classified devices or media will not be sent to a vendor for repair without prior approval from the local Security Office.

k. Use of Removal Storage Media (RSM). Use of non-DoD issued devices or media accessing government networks and computer systems is prohibited. Contractor procured devices and media must comply with the same hardware and physical security requirements to include classification labeling.

l. All compromised systems (i.e. malware/virus) will be blocked, and the user and Information Management Officer (IMO) will initiate and execute Command and/or local Incident Response Plan procedures. The system will not be granted network access until Information Assurance Manager (IAM) or Information Assurance Officer (IAO) reviews incident report, system has been wiped and re-imaged. The user will not be authorized to save any data on a compromised system unless data can be securely extracted from compromised system.

m. Violation of this policy will result in system isolation from the network and/or suspension of user privileges as indicated in the Acceptable Use Policy (AUP).

(1) First Offense. The violator's account will be suspended for a period of 30 working days. The violator will be required to retake the Cyber IA Awareness Challenge training, Portable Electronic Devices and Removable Storage Media, SAFE Home Computing, Social Media and Operations Security, and Army Specific Phishing training. Additionally, a memorandum signed by the first O-5 in the chain of command is required stating the following: the offense and the mitigating action the business unit will take to ensure the activity does not happen again. Only the Brigade Commander can exempt the 30-day suspension period.

(2) Second Offense. The violator's account will automatically be suspended indefinitely and will require a memo from the Brigade Commander to restore network access privileges.

7. The point of contact for this policy letter is the Brigade Signal Officer (S6) at DSN 315-722- 0824.

KRIS A. ARNOLD
COL, MI
Commanding

DISTRIBUTION:
A